William & Mary Business Law Review

Volume 4 | Issue 1 Article 7

Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach

John A. Fisher

SECURE MY DATA OR PAY THE PRICE: CONSUMER REMEDY FOR THE NEGLIGENT ENABLEMENT OF DATA BREACH

ABSTRACT

Every time we swipe our debit cards, pay our bills online, or sign up for a service like Netflix, we are entrusting important identifying information to the companies with which we do business. Most of the time, those companies take seriously the obligation to protect our data and prevent it from falling into the hands of those who would use it to benefit themselves at our expense. Some companies, however, fail to do enough to meet that burden, making it easier for identity thieves to inflict personal and financial injury on consumers. To date, our legal system has essentially denied consumers a remedy against these negligent businesses.

This Note seeks to explore the problem of data breach and offer solutions for both improving electronic data security and establishing a remedy for consumers. To elaborate on this problem, this Note examines two high-profile data breaches: the famous "TJX breach" and the more recent breaches suffered by the Sony Corporation. In both of these cases, millions of customers had their data exposed as a result of a failure to implement basic security protocols or update existing security models to incorporate advances in technology.

This Note will (1) examine the problem of data breach; (2) articulate means of establishing security standards for businesses; (3) argue for federal codification and regulation of those standards; and (4) argue that consumers should be empowered with a negligence cause of action, grounded in the theory of negligence per se, to hold businesses to those standards.

TABLE OF CONTENTS

INTRODUCTION

Consumers today entrust more data than ever before to the companies and organizations with which they do business. Credit card numbers, Social Security numbers, bank account information, and numerous other forms of personal and financial information are all entrusted to businesses during the course of the enormous number of transactions that occur each day. Often this information is stored on company servers, either as a courtesy to the customer or as a requirement of establishing a business relationship in anticipation of future transactions. Naturally, these databases of sensitive customer information present an attractive target to computer hackers. Often these hackers seek to steal the identities of consumers in order to engage in fraudulent transactions in their names. Increasingly, however, "hacktivists" seek to expose consumer data to get a business's attention, either to promote a particular cause, or to point out how vulnerable a particular business's network is to these kinds of cyber-attacks.[1] From a consumer's point of view, distinguishing between the identity thief and the hacktivist is virtually impossible, as once their data is exposed, identity theft is a concern regardless of the stated aim of the attackers.

In response, most companies seek to secure their networks that store vital consumer information through various means of electronic defenses such as firewalls, intrusion detection protocols, and authentication requirements.[2] In some cases, however, companies fail to take adequate steps to secure their customer data and their networks are breached, resulting in exposure of that data to those who gained access.[3] It is at this point, of "data breach" but no actual identity theft (i.e., fraudulent transactions), that consumers have suffered an injury for which our current legal system has, to date, denied them a remedy.[4]

---

[1] *See infra* note 17 and accompanying text.

[2] *See, e.g.*, *Discover Site Security Measures*, DISCOVER BANK, https://www.discover.com/credit-cards/member-benefits/security/online-safety/discover-site.html (last visited Feb. 2, 2013) (indicating that the Discover website utilizes "128-bit Secure Socket Layer (SSL)" encryption which "encodes information sent over the Internet" along with username and password requirements, firewalls, and intrusion detection systems).

[3] *See, e.g.*, Raj Chaudhary et al., *Have You Conducted a Data Protection Audit Lately?*, INTERNAL AUDITOR (Sept. 2011), http://www.theiia.org/intAuditor/feature-articles/2011/august/have-you-conducted-a-data-protection-audit-lately/.

[4] *See* Michael L. Rustad & Thomas H. Koenig, *Extending Learned Hand's Negligence Formula to Information Security Breaches*, 3 ISJLP 237, 264 (2007) [hereinafter Rustad & Koenig, *Extending*] ("No plaintiff has been successful in receiving an award to compensate for lost data where identity theft has not yet occurred.").

This Note argues that consumers should have a negligence cause of action in cases of data breach.[5] This cause of action should be grounded in a negligence per se theory based on federal codification of network security standards.[6] Part I will further elaborate the problem consumers and businesses face, focusing on the recent breaches Sony Corporation and its customers suffered related to its popular "PlayStation 3" entertainment system, along with the widely discussed case of *In re TJX Companies Retail Security Breach Litigation*.[7] Part II will highlight the fact that there is virtually no mandatory regulation of corporate network security in place today, discuss organizations that could serve as the source of standards for adequate network security, and argue that federal regulations should refer to or build upon those standards. Part III will discuss the traditional five elements of a negligence action: duty, breach, causation, harm, and damages. The negligence action available to consumers should be constructed along the lines of Professors Michael Rustad and Thomas Koenig's "negligent enablement of cybercrime,"[8] however it should be grounded in a negligence per se theory, calling upon the federal regulations discussed in Part II to establish a business's duty of care. This negligence action could be labeled "negligent enablement of data breach" and should incorporate Rustad and Koenig's toxic tort approach to data breach cases.[9] This approach would allow consumers to overcome the traditional hurdle they have faced in the courts—proving that they have actually suffered harm when no fraudulent transactions have been made with their information.[10] Part IV of this Note will conclude, offering caution that this problem needs to be addressed sooner rather than later, with the increasing prevalence of "cloud-computing."[11]

---

[5] *See id.* at 237; *see also* Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L.J. 1553, 1553 (2005) [hereinafter Rustad & Koenig, *The Tort*].

[6] BLACK'S LAW DICTIONARY (9th ed. 2009) (defining negligence per se as "negligence established as a matter of law, so that the breach of the duty is not a jury question. Negligence per se usu[ally] arises from a statutory violation.").

[7] *See In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 489 (1st Cir. 2009), *amended on reh'g in part* (D. Mass. 2009); *PSN News: Consumer Reports*, PLAYSTATION, http://us.playstation.com/news/consumeralerts/#us (last visited Feb. 2, 2013).

[8] *See generally* Rustad & Koenig, *The Tort*, *supra* note 5.

[9] *See* Rustad & Koenig, *Extending*, *supra* note 4, at 264–66.

[10] *Id.* at 266–70.

[11] *See IDC Predicts 2012 Will Be the Year of Mobile and Cloud Platform Wars as IT Vendors Vie for Leadership While the Industry Refines Itself*, INT'L DATA CORP. (Dec. 1, 2011), http://www.idc.com/getdoc.jsp?containerId=prUS23177411 (predicting that spending on "mobile computing, cloud services, social networking, and big data analytics technologies" would "account for at least 80% of IT spending growth between now and 2020").

I. THE PROBLEM OF DATA BREACH

A. Elaboration of the Problem

Data breach and the attendant risk of identity theft affect millions of Americans each year.[12] In 2011, there were 419 incidents of reported data breach resulting in the potential exposure of almost 23 million confidential records.[13]

Many of these reported data breaches are incidents of physical theft, such as the theft of a whole computer or its hard drive, or other physical data storage devices such as the ubiquitous "thumb drive."[14] Some of these data breaches are the result of negligent posting of private information onto publicly accessible areas of an organization's network.[15] However, the most problematic incidents of data breach are often a result of unauthorized intrusion into a business or other organization's data systems by cyberattackers, more commonly known as hackers.[16] In fact, hacking is increasingly seen not only as a way to steal funds or information with which to make fraudulent transactions, but also as a way of forcing a business to

---

[12] Jacob W. Schneider, Note, *Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data*, 15 B.U. J. SCI. & TECH. L. 279, 281–82 (2009) ("In recent years, the risk of identity theft has grown annually at a rapid rate. Between 2003 and 2006, the United States saw a fifty percent increase in the number of identity theft victims. Today, identity theft affects about fifteen million Americans each year." (footnotes omitted)).

[13] *2011 ITRC Breach Report*, IDENTITY THEFT RES. CTR. (Feb. 7, 2012), http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_2011_20120207.pdf.

[14] For example, a drive containing over 63,000 personal records was stolen from the vehicle of "an employee of Neurological Institute of Savannah & Center for Spine." *Id.* at 14.

[15] *See id.* at 29 ("Yale University has notified about 43,000 faculty, staff, students and alumni that their names and Social Security numbers were publicly available via Google search for about 10 months."). The data breach at Yale was evidently the result of the decision to store unencrypted personal information on a publicly accessible FTP (File Transfer Protocol) server that Google's automated processes eventually accessed and incorporated into their search results. *See* Jaikumar Vijayan, *Yale Warns 43,000 About 10-Month-Long Data Breach*, COMPUTERWORLD (August 22, 2011, 4:54 PM), http://www.computerworld.com/s/article/9219369/Yale_warns_43_000_about_10_month_long_data_breach.

[16] *See 2011 ITRC Breach Report Key Findings*, IDENTITY THEFT RES. CTR. (Mar. 10, 2011), http://www.idtheftcenter.org/artman2/publish/headlines/Breaches_2011.shtml (accessed by searching the Internet Archive index) (noting that "[h]acking attacks were responsible for more than one-quarter (25.8%)" of 2011 data breaches, "hitting a five-year all time high") (footnote omitted); *see also 2011 ITRC Breach Report*, IDENTITY THEFT RES. CTR., *supra* note 13, at 20 ("Betfair says cyberattackers likely gained access to the credit and debit details affiliated with *2.3 million* customers.") (emphasis added).

take notice of your cause.[17] From a consumer point of view, however, distinguishing between hacktivists and other hackers who intend to access consumer personal information for their own gain is virtually impossible, and largely academic. Once their information is exposed, the threat of subsequent identity theft, whether by a rogue member of a hacktivist group or by a hacker whose goal was theft all along, hangs over the heads of all data breach victims.

B. High Profile Examples of Data Breach: Sony PlayStation and TJX

All of the above types of data breach are troubling, not only because of the sheer volume of sensitive personal information exposed, but also because of the fact that such incidents could often have been ameliorated or even entirely avoided by employing a minimal amount of modern information security practices.[18] Two stark examples of such failures are the events leading to the oft-discussed case of *In re TJX Companies Retail Security Breach Litigation*[19] and the more recent attack on Sony Corporation's "PlayStation Network," serving its popular "PlayStation 3" entertainment system.[20]

The facts of *TJX* represent the worst-case scenario for data breach. Beginning in 2005 and continuing for 18 months, hackers went undetected as they accessed TJX's databases, exposing "at least 45 million credit and debit cards to potential fraud."[21] It was eventually discovered that the hackers gained access to TJX's systems by intercepting a retail store's wireless communications containing information that allowed the hackers to gain access to TJX's central database.[22] These hackers were able to accomplish this intrusion with relative ease, due to the fact that TJX was using an outdated

---

[17] *See* Ravi Somaiya & Steve Lohr, *Arrest Puts Spotlight on Brazen Hacking Group LulzSec*, N.Y. TIMES, June 23, 2011, http://www.nytimes.com/2011/06/24/technology/24hack.html ("[T]he actions of LulzSec fall broadly into the category known as hacktivism. Hackers of this type are not motivated by money, but are mainly interested in protesting against or antagonizing their targets .... Hacktivists tend to portray their activities as digital sit-ins, a form of protest.").

[18] *See* Vijayan, *supra* note 15. Had Yale at least encrypted the data stored on their publicly accessible server, even though the files would have still been downloadable by outsiders, they would have been much harder to actually open and read.

[19] *In re* TJX Cos. Retail Sec. Breach Litig., 564 F.3d 489, 489 (1st Cir. 2009), *amended on reh'g in part* (May 5, 2009).

[20] *See PSN News: Consumer Alerts*, PLAYSTATION, *supra* note 7.

[21] Mark Jewell, *Encryption Faulted in TJX Hacking*, MSNBC.COM (Sept. 25, 2007), http://www.msnbc.msn.com/id/20979359/ns/technology_and_science-security/t/encryption-faulted-tjx-hacking/#.Tqxz2kMg_m0.

[22] Joseph Pereira, *Breaking the Code: How Credit-Card Data Went Out Wireless Door*, WALL ST. J., May 4, 2007, at A1.

form of wireless security[23] and had failed to take additional security measures, such as the installation of firewalls.[24] In fact, the hackers "were so confident of being undetected that they left encrypted messages to each other on the company's network, to tell one another which files had already been copied and avoid duplicating work."[25] For consumers however, the problems went beyond the mere theft of their confidential and personal data. It eventually became known that the hackers were selling consumer financial data to gangs of thieves, who used that information to make fraudulent purchases.[26]

More recently, in the summer of 2011, Sony Corporation and many of its subsidiaries were the targets of numerous hacking incidents.[27] Most notably, hackers brought down the online component of Sony's popular PlayStation 3 entertainment console for approximately one month.[28] Sony confirmed that name, address, country, email address, birth date, logins (usernames and associated passwords), and other data may have been obtained during the breach, and hinted at the possibility that credit card data was also obtained in the attack.[29] The breach affected over 75 million accounts across the world.[30] It appears likely that hacktivist group "Anonymous" was involved in the attack.[31] As of October 2012, class action litigation

---

[23] *Id.* at A12 (explaining how TJX was using "a flawed encoding system called Wired Equivalent Privacy, or WEP" at a time when "the wireless industry was offering a more secured system called Wi-Fi Protected Access or WPA, with more complex encryption").

[24] *Id.*

[25] *Id.*

[26] For example, one gang, "using bogus credit cards stolen from hundreds of TJX customers ... bought $8 million worth of gift cards and used them to buy flat-screen TVs, computers and other electronics." *Id.*

[27] *See PSN News: Consumer Alerts*, PLAYSTATION, *supra* note 7; *see also Sonypictures.com Data Security Incident*, SONY PICTURES (June 8, 2011), http://www.sonypictures.com/corp/consumeralert.html.

[28] *See PSN News: Consumer Alerts*, PLAYSTATION, *supra* note 7 (notifying consumers of the breach and the shutdown of the network between April 17th and 19th); Daniel Ionescu, *Green Light Is On—Sony PlayStation Network Returns in US*, PCWORLD (May 15, 2011, 9:46 AM), http://www.pcworld.com/article/227917/green_light_is_on_sony_playstation_network_returns_in_us.html.

[29] *See PSN News: Consumer Alerts*, PLAYSTATION, *supra* note 7 ("While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility.").

[30] Emily Chung, *PlayStation Data Breach Deemed in 'Top 5 Ever*,*'* CBC NEWS (Apr. 27, 2011, 10:56 AM), http://www.cbc.ca/news/business/story/2011/04/27/technology-playstation-data-breach.html.

[31] Nick Bilton, *Sony Explains PlayStation Attack to Congress*, N.Y. TIMES BITS BLOG (May 4, 2011, 12:59 PM), http://bits.blogs.nytimes.com/2011/05/04/sony-responds-to-lawmakers-citing-large-scale-cyberattack/ ("Although Sony said [in a letter to Congressional Representative Mary Bono Mack] it did not know who was responsible for the

does not look promising in terms of providing relief for the affected class of PlayStation Network users.[32]

Unfortunately for Sony and its customers, the PlayStation Network was not the only Sony asset that suffered a data breach in 2011. In June of 2011, Sony Pictures Entertainment was attacked, compromising the personal information of approximately 37,500 individuals.[33] This time, Sony was clear that the stolen data did not contain "any credit card information, social security numbers or driver license numbers."[34] Troubling, however, is the suggestion by the hackers themselves "that Sony had stored its users' information, including passwords, in plain text, with no encryption whatsoever."[35]

Both TXJ and Sony point out the danger consumers face when companies fail to take the proper steps to secure networks holding their data. The Sony breach in particular highlights the need for companies to plan their security with the assumption that there will be a breach at some point in time. Companies need to keep sensitive consumer data stored in encrypted formats so that if hackers do gain access, the data they obtain will be much harder for them to use. *TJX*, on the other hand, shows just how much consumer data can be exposed by a failure to keep up with evolving security standards.

II. SETTING SECURITY STANDARDS

It is important to understand that though Sony and TJX may have failed to implement necessary data security measures, in our current system, they may not be entirely to blame for that failure. This is because network and data security standards are mostly developed either by private organizations[36] or

---

attacks, the letter said the company believed a group called Anonymous played a role, as Sony found files on its servers that said 'Anonymous' and 'We Are Legion.'").

[32] *See* Lucile Scott, *Judge Dismisses Much of PlayStation Hacking Suit*, COURTHOUSE NEWS SERVICE (2012), https://www.courthousenews.com/2012/10/19/51486.htm (discussing District Judge Anthony Battaglia's dismissal of many of the class claims, including the bailment claim, which was dismissed on the grounds that "plaintiffs freely admit, plaintiffs' personal information was stolen as a result of a criminal intrusion of Sony's Network").

[33] *See* SONY PICTURES, *supra* note 27.

[34] *Id.*

[35] Nick Bilton, *New Questions as Sony Is Hacked Again*, N.Y. TIMES BITS BLOG (June 8, 2011, 7:30 AM), http://bits.blogs.nytimes.com/2011/06/08/new-questions-as-sony-is-hacked-again/.

[36] *See* Software Eng'g Inst., Carnegie Mellon, *The CERT® Program FAQ*, CERT, http://www.cert.org/faq/cert_faq.html (last updated June 20, 2012) ("The CERT Program is an organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems ...."); *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*, PCI SEC. STANDARDS COUNCIL 5 (Oct. 2010), https://www.pcisecuritystandards.org/documents

by non-regulatory government agencies.[37] Thus, companies (at least in most fields)[38] are not required to implement or even stay up to date with evolving data security practices.[39] To adequately protect consumers and avoid situations like Sony, TJX, and the hundreds of other data breaches that occur each year, something must be done to motivate companies to pay attention to and implement such standards within their own security plans.

This Note proposes a mixture of government, private, and consumer cooperation to accomplish this goal. The result would give consumers the power to hold accountable those companies that fail to properly secure their personal information. First, we need uniform federal legislation that incorporates the work of private organizations and non-regulatory government agencies in the data security field.[40] Such legislation would be self-updating by simply referring to the work of these organizations and agencies as the requisite standard.[41] Then, under a theory that companies who implement lax data security measures are engaging in unfair or deceptive acts or practices,[42] the Federal Trade Commission (FTC) could police compliance with these standards.[43] This does little, of course, to

---

/pci_dss_v2.pdf ("PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data.").

[37] *See Computer Security Division*, NAT'L INST. OF STANDARDS AND TECH., http://nist.gov/itl/csd/index.cfm (last updated Jan. 18, 2013) ("The Computer Security Division (CSD), a component of NIST's Information Technology Laboratory (ITL), provides standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services."). NIST is a non-regulatory agency. *NIST General Information*, NAT'L INST. OF STANDARDS AND TECH., http://www.nist.gov/public_affairs/general_information.cfm (last updated May 31, 2012).

[38] *See infra* notes 50–53 and accompanying text.

[39] *See* Michael E. Jones, *Data Breaches: Recent Developments in the Public and Private Sectors*, 3 ISJLP 555, 570 (2008) ("Currently no relevant federal legislation concerning data breaches involving private entities has passed Congress."); Robert Sprague & Corey Ciocchetti, *Preserving Identities: Protecting Personal Identifying Information Through Enhanced Privacy Policies and Laws*, 19 ALB. L.J. SCI. & TECH. 91, 137 (2009) ("Though nearly all the states have enacted data breach notification laws that promote data encryption, companies are only obligated to *notify* individuals if their unencrypted PII [Personal Identifying Information] has been the subject of unauthorized disclosure." (emphasis added)).

[40] *See infra* Part III.

[41] *But see* Abraham Shaw, Note, *Data Breach: From Notification to Prevention Using PCI DSS*, 43 COLUM. J.L. & SOC. PROBS. 517, 558–59 (2010) (proposing that "legislatures should strive to codify the security principles embodied in PCI DSS, rather than requiring specific technology, to avoid having to constantly update the law"). Shaw's argument fails to take into account that some attacks can only be prevented by specific types or configurations of hardware and software. WPA wireless encryption, for example, requires a hardware router that is capable of providing that level of encryption.

[42] *See* 15 U.S.C. § 45 (2006); *see also* Shaw, *supra* note 41, at 538.

[43] The FTC is already pursuing this theory but only *after* breaches occur. Shaw, *supra* note 41, at 538–42.

protect consumers who suffer when a company is breached *before* the FTC detects its lax security measures. In such cases, consumers should be able to refer to this robust legislation as the basis for a negligence per se action against the company.

A. Existing State and Federal Efforts

Existing state efforts to combat the problem of data breach focus overwhelmingly on notification.[44] State notification laws require businesses "to publicly acknowledge data breaches, alerting affected parties to take appropriate precautions."[45] Such laws only allow for civil action if a consumer suffers injury because of a company's failure to notify under the statute, not for injury stemming from the underlying data breach.[46] Many states have used the notification statute adopted by California as a model for their own notification law.[47] As a result, most states follow California in carving out an exception to the notification requirement, allowing breached companies to avoid notifying affected consumers "when the lost data was encrypted (as opposed to plain-text) or to assist law enforcement."[48] Importantly, many states also follow California's example in declaring waiver of notification contrary to public policy and therefore void and unenforceable.[49] This prevents consumers from unwittingly giving up their right to notification when entering into contractual relationships with companies.

At the federal level, there is currently no broadly applicable uniform legislation that governs data security and notification.[50] The statutes that do exist only apply to specific situations or fields, such as the Health Insurance Portability and Accountability Act (HIPAA) in healthcare,[51] or the Gramm-Leach-Bliley Act (GLBA) in the financial services industry.[52] The GLBA, as enhanced by the FTC's "safeguard rule,"[53] represents a step in the right

---

[44] *See* Schneider, *supra* note 12, at 282 ("With data breach incidents on the rise, forty-four states have enacted notification statutes.").

[45] *Id.*

[46] Sprague & Ciocchetti, *supra* note 39, at 105; *see also* CAL. CIV. CODE § 1798.84(b) (West 2012).

[47] Schneider, *supra* note 12, at 282–83.

[48] *Id.* at 283.

[49] *See, e.g.*, CAL. CIV. CODE § 1798.84(a) (West 2012).

[50] Shaw, *supra* note 41, at 534; *see also* Sprague & Ciocchetti, *supra* note 39, at 137 ("For non-financial web-based activities and transactions there are no direct legal restrictions on what companies can do with [Personal Identifying Information] they collect—particularly the manner in which PII is stored.").

[51] 45 C.F.R. §§ 164.312, 164.502 (2011).

[52] Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., and 16 U.S.C.).

[53] *See* Shaw, *supra* note 41, at 537.

direction because it requires financial institutions to secure customer information and notify customers in the event of a breach.[54] Aside from being applicable only to the financial services industry (and businesses dealing with that industry), the GLBA as enhanced by the safeguard rule falls short as an ideal uniform regulation because it fails to provide companies with any concrete standards, such as particular hardware to install or particular security protocols to employ, to ensure customer data is secure.

B. Sources of Security Standards

One place companies and other organizations could turn to for such standards is the Computer Security Division (CSD), a component of the National Institute of Standards and Technology's (NIST) Information Technology Laboratory (ITL).[55] The CSD's security research focuses on "emerging technologies" and "new security solutions that will have a high impact on the critical information infrastructure."[56] The CSD "[e]valuate[s] security policies and technologies from the private sector and national security systems for Federal agency use" and compiles its research into "a specification for minimum security requirements for Federal information and information systems."[57] Naturally, the CSD's work is primarily utilized by the federal government.[58]

Another source for computer security standards is Carnegie Mellon University's CERT program. CERT "is an organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems."[59] The CERT program is federally funded,[60] and as a result, "the majority of [its] work contributes to government and national security efforts."[61] Importantly, however, CERT publishes many of its tools in an open source format, meaning any organization can make use of or even improve upon CERT's work.[62] These tools include methods for "discovering vulnerabilities, analyzing network traffic, and

---

[54] *Id.*

[55] *See Computer Security Division*, NAT'L INST. OF STANDARDS AND TECH., *supra* note 37.

[56] *Systems & Emerging Technologies Security Research*, COMPUTER SEC. DIV., COMPUTER SEC. RES. CTR., http://csrc.nist.gov/groups/SNS/ (last visited Feb. 2, 2013).

[57] *About CSD*, COMPUTER SEC. DIV., COMPUTER SEC. RES. CTR., http://csrc.nist.gov/about/index.html (last visited Feb. 2, 2013).

[58] *Id.*

[59] *See* Software Eng'g Inst., *The CERT® Program FAQ*, CERT, *supra* note 36.

[60] *See id.*

[61] Software Eng'g Inst., Carnegie Mellon, *About Us*, CERT, http://www.cert.org/meet_cert (last updated Nov. 15, 2011).

[62] *Id.*

facilitating digital investigations," allowing organizations to improve their security by "identifying information security gaps, improving resilience, and measuring susceptibility to insider threat."[63]

The research conducted by organizations like the CSD and CERT is invaluable in staying up-to-date with the fast moving target of computer and network security. Legislative efforts like Gramm-Leach-Bliley need to incorporate the work of these groups, so that organizations have some reference point for securing the data they hold, and so that enforcement efforts, such as those conducted by the FTC, have a framework for assessing data security. A good example of what this kind of legislation might look like can be found in the privately crafted "Payment Card Industry (PCI) Data Security Standard."[64]

C. Payment Card Industry Data Security Standard (PCI DSS)

The PCI DSS is developed and updated by the PCI Security Standards Council, an organization founded in 2006 by the major payment card companies: American Express, Discover, JCB International, MasterCard, and Visa.[65] PCI DSS was "developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements to protect cardholder data."[66] The document "requires all retailers, online merchants, data processors, and other businesses that handle credit card information" to follow its security and assessment procedures.[67]

The "high-level overview" of the DSS outlines twelve requirements, including "install and maintain a firewall configuration to protect cardholder data" and "encrypt transmission of cardholder data across open, public networks."[68] Importantly, the document also tells participating entities *how* to accomplish these requirements. For example, the use of WEP encryption to secure wireless communications (the same encryption TJX had in place when it suffered its data breach) is expressly prohibited by the PCI DSS.[69]

---

[63] *Id.*

[64] *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*, PCI SEC. STANDARDS COUNCIL, *supra* note 36, at 5.

[65] *About Us*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/organization_info/index.php (last visited Feb. 2, 2013).

[66] *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*, PCI SEC. STANDARDS COUNCIL, *supra* note 36.

[67] *See* Rustad & Koenig, *The Tort*, *supra* note 5, at 1588.

[68] *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*, PCI SEC. STANDARDS COUNCIL, *supra* note 36, at 20, 35.

[69] *Id.* at 36.

III. CODIFICATION AND ENFORCEMENT

Perhaps because it is not mandatory,[70] some scholars caution that the PCI DSS is really an example of industry custom and "is a good test for reasonable care only when industry practices do not create unreasonable preventable dangers."[71] The concern here seems to be with the (at the time) relatively undeveloped standards and best practices of the industry.[72] As it stands today, however, the PCI DSS represents more than industry custom. It stands as a model for the federal government to refer to in constructing comprehensive legislation, applicable to all companies and organizations that deal with consumer data. Such legislation would outline both detailed technical requirements and general security principles[73] that are updated and informed by the work of agencies such as the CSD and groups such as CERT.

A. Federal, Not State

From a consumer protection standpoint, it is important that data security standards be set at the federal level, rather than by individual states. Arguments for state standards focus on the states' traditional laboratory functions and their history of leading the way in this area with notification laws.[74] It has been suggested that "state-created notification laws have effectively created a race to the top," with companies constructing their security plans in accordance with the toughest state laws.[75]

These arguments fail to take into account that a race to the top for companies creates a race to the bottom for those seeking to breach a company's networks. Variations in state laws inevitably result in some states with weaker standards. If a company primarily does business in a state with weaker data security standards, it may wish to avoid the tougher requirements of states in which it does not conduct business, and satisfy only the weaker standards. This naturally creates an incentive for hackers and other cybercriminals to target companies in these weaker states. This

---

[70] Compliance with the PCI DSS is voluntary and often encouraged through financial and operational incentives or consequences put forth by the payment card companies. *See For Merchants*, PCI SEC. STANDARDS COUNCIL, https://www.pcisecuritystandards.org/merchants/index.php (follow "What are the consequences to my business if I do not comply with the PCI DSS?" hyperlink) (last visited Feb. 2, 2013).

[71] Rustad & Koenig, *The Tort*, *supra* note 5, at 1589.

[72] *See id.*

[73] *See* Jones, *supra* note 39, at 570.

[74] *See* Shaw, *supra* note 41, at 550–52.

[75] *Id.* at 550.

would lead to a disproportionate number of data breaches affecting those consumers unfortunate enough to do business with such companies, even though the companies may be following the applicable laws.

Furthermore, companies and other organizations need clear guidance on what exactly they need to do in order to secure consumer data, and consumers need a clear benchmark for assessing whether they want to entrust those entities with their information.[76] A uniform federal law would satisfy both of those interests in a more efficient way than a myriad of state standards.

B. Enforcement and Accountability

As mentioned above in Part II, one way companies are currently held accountable for data breaches is through FTC enforcement actions.[77] Generally, the FTC relies on section 5 of the Federal Trade Commission Act,[78] a section that prohibits unfair and deceptive acts or practices.[79] The cases in which the FTC has employed this theory suggest that the FTC is concerned with at least five inadequate data security practices:

> (1) inadequately assessing system vulnerability to commonly known or reasonably foreseeable attacks;
> (2) failing to apply low-cost, simple, and readily available defenses;
> (3) using default user ID or passwords to protect sensitive data rather than stronger passwords to prevent hackers;
> (4) storing information in unencrypted files and sending sensitive data via unencrypted transmission routes; and
> (5) failing to develop unauthorized access detection mechanisms.[80]

Currently, the FTC brings an enforcement action alleging that the breached company "failed to provide reasonable and appropriate security for the consumer information stored on their network, including credit card numbers, expiration dates, and security codes."[81] Often, the company

---

[76] *But see id.* (arguing that the perceived "race to the top" shows companies have had no problem "navigating the maze of state laws to ensure compliance").

[77] *See supra* notes 40–42 and accompanying text; Sprague & Ciocchetti, *supra* note 39, at 138–40.

[78] 15 U.S.C. § 45 (2006).

[79] *See* Shaw, *supra* note 41, at 538–42 (discussing current FTC enforcement efforts).

[80] *Id.* at 542 (citing Joel B. Hanson, Note, *Liability for Consumer Information Security Breaches: Deconstructing FTC Complaints and Settlements*, 4 SHIDLER J.L. COM. & TECH. 11 (2008)).

[81] Sprague & Ciocchetti, *supra* note 39, at 138 (citing Amended Consolidated Class Action Complaint at para. 8, *In re* Life is Good, Inc. (F.T.C. 2007) (No. 072-3046), http://www.ftc.gov/os/caselist/0723046/080117complaint.pdf).

then signs a consent agreement in which it agrees to "establish and implement, and thereafter maintain a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers."[82]

As Robert Sprague and Corey Ciocchetti point out, "[t]he one element missing in the FTC complaints and agreements are penalties for non-compliance."[83] Additionally, the discussion in Part II highlights that both companies and consumers need more than nebulous directives to companies that they secure sensitive data. Both need concrete standards by which to assess the strength of security implementations (or lack thereof).[84]

More importantly, enforcing data security standards only after a breach is simply too late.[85] The better approach, in terms of securing consumer data, is to have the FTC monitor these companies for compliance with uniform federal data security standards *before* a breach occurs. Naturally, however, there remains a gap where data breach can occur before the FTC has detected non-compliance. It is at this point that consumers should also be able to make use of uniform federal data security standards legislation by bringing negligence per se actions against non-compliant companies.

IV. NEGLIGENCE CAUSE OF ACTION

The idea of providing consumers with a negligence cause of action in cases of data breach is relatively new. In 2005, Professors Michael L. Rustad and Thomas H. Koenig proposed "a new tort of negligent enablement" directed at software venders that produce "defective products and services that pave the way for third party cybercriminals who exploit known vulnerabilities."[86] Rustad and Koenig outlined all the traditional elements of a negligence cause of action[87] and even briefly discussed how their proposed tort would fit into a negligence per se framework.[88] The negligence per se cause of action proposed in this Part will proceed from Rustad and Koening's basic description of the elements and tailor those elements to the kind of data breach described in Part I, while also incorporating the proposed statutory backbone of Parts II and III.

---

[82] *Id.* (citing Agreement Containing Consent Order at para. 3, *In re* Life is Good, Inc. (F.T.C. 2007) (No. 072-3046), http://www.ftc.gov/os/caselist/0723046/080117agreement.pdf).

[83] *Id.* at 139.

[84] *See* Shaw, *supra* note 41, at 550–52.

[85] *See* Shaw, *supra* note 41, at 538.

[86] Rustad & Koenig, *The Tort*, *supra* note 5, at 1553.

[87] *See id.* at 1586–1610.

[88] *See id.* at 1592.

A. Duty

At this point, the duty that should be required of businesses that deal with sensitive consumer data should be clear. Similar to the existing duty implicit in the FTC enforcement actions,[89] businesses should have a legal duty to take reasonable care to protect sensitive consumer information from unauthorized access.[90] As with the duty element of any negligence cause of action, one concern here is with the term "reasonable care."[91] Since this Note seeks to ground the cause of action in a negligence per se theory, clarifying the term "reasonable care" as it applies to a company's security policies and implementation is straightforward. Anything that falls below the standards set by the kind of uniform federal legislation called for in Parts II and III[92] will fail to constitute reasonable care.

The more interesting problem, however, is one shared by all negligence causes of action. Just as some slips and falls are not reasonably foreseeable, theoretically there is the possibility of a data breach that no one could have reasonably predicted at the time. As Rustad and Koenig correctly note, "[a]ny duty to protect computer users from the cybercrimes of third persons must be predicated on a preventable risk."[93] This means that businesses should not have a duty to guard against innovative breaches that have no known or effective defense at the time of the attack.[94] Here

---

[89] *See* Shaw, *supra* note 41, at 542.

[90] *See* Rustad & Koenig, *Extending*, *supra* note 4, at 239–40 ("We argue that companies have a duty to provide reasonable information security practices under the common law of torts."); Sprague & Ciocchetti, *supra* note 39, at 140–41 ("Ultimately, companies *must* design, implement, and maintain adequate security programs to protect PII." (emphasis added)).

[91] BLACK'S LAW DICTIONARY defines reasonable care "[a]s a test of liability for negligence, the degree of care that a prudent and competent person engaged in the same line of business or endeavor would exercise under similar circumstances." BLACK'S LAW DICTIONARY 240 (9th ed. 2009).

[92] *See supra* Part II.A–B; see also *infra* Part IV.B for a discussion of how the material discussed in Parts II and III can be synthesized into a workable statute upon which to base a negligence per se cause of action.

[93] Rustad & Koenig, *The Tort*, *supra* note 5, at 1587; *see also* Rustad & Koenig, *Extending*, *supra* note 4, at 251 ("The duty to implement security thwarting third-party cybercrimes should turn on whether the crime was foreseeable.").

[94] The instances of such indefensible breaches are rare. This is likely due to the overlapping nature of security systems. For example, in December of 2011, Columbia researchers discovered a vulnerability in HP LaserJet printers that "could allow hackers to remotely control printers over the internet." Kevin Parrish, *HP Issues Firmware to Address Printer Vulnerability*, TOM'S GUIDE (Dec. 28, 2011, 6:00 AM), http://www.tomsguide.com/us/Columbia-University-HP-LaserJet-Printer-Exploit,news-13671.html. HP acknowledged the vulnerability but indicated that "no customer [had] reported unauthorized access." *Id.* This is likely due to the fact that a basic firewall (present in virtually all home routers and requiring little to no user interaction to ensure protection) would protect against the attack. *Id.*

too, grounding this action in negligence per se affords some aid to both consumers seeking relief, and courts seeking to adjudicate post-data breach claims. In addition to setting a security standards floor, constructing legislation centered on the work of agencies like the CSD and organizations like CERT[95] also provides a measure of what it means for an attack to be innovative enough to fall outside the reasonableness standard. If an attack is so new that not even computer security experts could have anticipated it, absent further negligence on the part of the breached company,[96] one should be extremely hesitant in holding that company liable for the breach.[97]

More importantly, the notion that businesses only have a duty to guard against foreseeable risks of data breach places a burden on consumers to guard against breach as well. Consumers should take the time to evaluate the security policies of the specific companies with which they do business online and understand good Internet security practices in general.[98] In the short term this may lessen the incidence of "phishing" attacks, in which unwary users are lured into putting sensitive information (such as bank login usernames and passwords) into fake sites posing as the legitimate site the user is trying to access.[99] For example, many sites use a form of Internet security known as "Hypertext Transfer Protocol Secure" (HTTPS).[100] To put it simply, HTTPS is a means of securing online communications between

---

[95] *See supra* Part II.B.

[96] For example, if a cybercriminal is able to make use of something like the vulnerability in the HP printers in a corporate setting, a consumer would still have a negligence cause of action under the theory proposed by this Note. The argument would be that the company failed to properly configure their firewall to protect against the possibility that other systems on their network (such as the flawed printer, or more likely, a server housing consumer data) may be vulnerable.

[97] This may seem unfair to consumers, as they are forced to bear the loss for something no one could have foreseen. It may be a moot point however because, as indicated above, such incidents should be incredibly rare. *See supra* Part II.B.

[98] *See* Sprague & Ciocchetti, *supra* note 39, at 136 ("Consumers should possess at least some of the responsibility for learning as much as they can about any website that requires their PII submissions.").

[99] BLACK'S LAW DICTIONARY defines phishing as "[t]he sending of a fraudulent electronic communication that appears to be a genuine message from a legitimate entity or business for the purpose of inducing the recipient to disclose sensitive personal information." BLACK'S LAW DICTIONARY 1263 (9th ed. 2009).

[100] For an in-depth explanation, see *Beginners Guide to SSL Certificates: Making the Best Choice When Considering Your Online Security Options*, VERISIGN (2010), http://www.verisign.com/ssl/ssl-information-center/ssl-resources/guide-ssl-beginner.pdf. VeriSign, now part of Symantec, makers of the popular Norton Antivirus, is a massive player in the online security business, responsible for providing validation services for over 4.5 billion daily hits. SYMANTEC, https://www.symantec.com/ssl-certificates (follow "Advantages" tab) (last visited Feb. 2, 2013).

a consumer's Internet browser and a company's website.[101] If a hacker intercepts the communication, he or she will be hard-pressed to access the information it contains.[102] In that way, HTTPS is similar in concept to using a code language that only you and a friend know to exchange traditional paper correspondence. Consumers can easily identify websites that utilize HTTPS by looking for a small padlock,[103] or for part of the website's name to be highlighted in green.[104] If a consumer knows their financial site is supposed to utilize HTTPS, yet they do not see the padlock or green text, then they will know that they are being targeted for a phishing scam. Alternatively, if the consumer knows the site they are on is legitimate, yet they do not see any indication that the site utilizes HTTPS, then they know the site is not secure and they should not communicate their sensitive information.

The burden on consumers to educate themselves and implement good Internet security practices is not meant as a device for allowing businesses to shrug off their duty of care. Quite the opposite, the burden on consumers should provide greater incentive to businesses to discover risks and notify consumers of them, so as to be able to make the argument that consumers should have been aware of the danger.[105] For example, should a company discover that impersonating emails are being sent to consumers directing them to fraudulent sites in an attempt to steal their information, the company should immediately send out an alert to all potential victims.[106] If after receiving this notice (and assuming no other negligence on the part of the company), a consumer falls victim to the scam anyway, the company should not be held liable for the consumer's failure to do his or her own part in securing their data.

---

[101] *Beginner's Guide to SSL Certificates*, VERISIGN, *supra* note 100, at 4.

[102] *See HTTPS*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/https (last visited Feb. 2, 2013). The Electronic Frontier Foundation (EFF) is a nonprofit organization that holds itself out as "confront[ing] cutting-edge issues defending free speech, privacy, innovation, and consumer rights today" in the online world. *About EFF*, ELEC. FRONTIER FOUND., https://www.eff.org/about (last visited Feb. 2, 2013).

[103] *Beginner's Guide to SSL Certificates*, VERISIGN, *supra* note 100, at 3.

[104] *Id.*

[105] At least one commentator sees this kind of increased incentive as a cause for concern. *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 263–64 (2007) ("Even if the result is economic waste, actors might adopt excessive, and perhaps inefficient, precautions in a negligence regime in order to bolster their claim to have exercised due care should litigation arise."). This is exactly the kind of effort we want to encourage because of the rapidly changing nature of technology and the diligence of cybercriminals.

[106] For an example of this practice in the federal government, see *Consumer Alerts*, FED. DEPOSIT INS. CORP., http://www.fdic.gov/consumers/consumer/alerts/ (last updated Jan. 30, 2013).

At this point, it should be mentioned that the classic Hand formula[107] is an inappropriate method to establish duty in this context.[108] One fear with the use of the Hand formula is that it would "deter businesses from engaging in electronic commerce altogether."[109] Practically speaking, all the Hand formula provides in this context is a dollar amount that companies should be spending on network security to avoid liability. Because of the high potential for data breach[110] and the likelihood of high resulting damages,[111] that figure may be more than even the wealthiest companies could afford.[112] Furthermore, the Hand formula provides no real guidance to actually securing a network, beyond throwing as much money as possible at the problem.

B. Breach

As indicated throughout this Note, breach should be determined on a negligence per se theory.[113] Rustad and Koenig viewed negligence per se as a possibility in creating their tort of negligent enablement of cybercrime in the software context.[114] They discuss three factors for determining whether adopting a statute as the standard of care is appropriate: "(1) Does the statute provide specific guidance on the standard of care? (2) Was the

---

[107] *See* United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947) (presenting the formula as B<PL where B equals "the burden of adequate precautions," P equals the probability of harm, and L equals "the gravity of the resulting injury").

[108] For a discussion of the Hand formula in the electronic security context, see Rustad & Koenig, *Extending*, *supra* note 4, at 239–40 (arguing that "[t]he best analytical approach for crafting this new duty involves determining whether the burden of a comprehensive security solution is less than the magnitude of the damages caused by lost or stolen data, multiplied by the probability of occurrence."). *But see* Schneider, *supra* note 12, at 298–300 ("The usefulness of this formula in data breach cases depends on our ability to estimate its variables properly.").

[109] Schneider, *supra* note 12, at 299–300 (fearing that "the Hand Formula would yield the same result as imposing strict liability").

[110] *See id.* at 299 ("Nearly one in four Americans will have their data exposed each calendar year." (citing Steve Lohr, *Surging Losses, but Few Victims in Data Breaches*, N.Y. TIMES, Sept. 27, 2006, http://www.nytimes.com/2006/09/27/technology/circuits/27lost.html)).

[111] *See* Schneider, *supra* note 12, at 299–300.

[112] This explains Schneider's fear of the Hand formula essentially imposing strict liability. *See id.* Since no one could ever afford to pay as much for data security as the Hand formula would require, in virtually every case the company would be found negligent and the cause of action would fail to guide or promote conduct in any meaningful way.

[113] *See supra* note 6 and accompanying text.

[114] *See* Rustad & Koenig, *The Tort*, *supra* note 5, at 1593–94 ("If statutes were enacted specifying a given level of computer security, users could use the violation of that statutory standard of care as a potent surrogate for negligence.").

statute enacted to protect against the harm suffered by the plaintiff? and (3) Was the plaintiff included in the class protected by the statute?"[115]

Then, as now,[116] "there [was] little by way of legislative guidance on what constitutes reasonable security."[117] The PCI Security Standards Council was in its infancy[118] and the PCI DSS was just emerging as a model on which to base the kind of legislation needed for a negligence per se cause of action.[119] As seen in Parts II and III, the PCI DSS is now well-established.[120] When continually updated with research from the other organizations described in Part II,[121] and supplemented by the federal enforcement efforts described in Part III,[122] the legislation that emerges is exactly the kind of legislation that meets Rustad and Koenig's three criteria.[123] Such legislation would certainly provide guidance on the standard of care companies would need to meet to guard consumer data; indeed, the PCI DSS as it exists now already provides exactly this sort of guidance.[124] The statute could easily be enacted to directly address the problem of data breach, as opposed to trying to fit the negligence per se action under some other statute such as HIPPA or the GLBA.[125] Finally, since the statute would outline what companies needed to do to secure consumer data, consumers would have no trouble in successfully arguing that they were encompassed by the statute's protection. This provides support that a negligence per se action is sustainable under such a legislative regime. Under this theory, consumers could establish breach by pointing to a company's failure to comply with the standards set forth in the adopted legislation.

---

[115] *Id.* at 1593.

[116] *See supra* Part II.B.

[117] Rustad & Koenig, *The Tort*, *supra* note 5, at 1593.

[118] *See supra* notes 62–63 and accompanying text.

[119] Version 1.1 of the PCI DSS was released in September of 2006. *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*, PCI SEC. STANDARDS COUNCIL, 1 (Sept. 2006), https://www.pcisecuritystandards.org/documents/pci_dss_v1-1.pdf; *see also supra* Part II.C. PETER SILVA, COMPLYING WITH PCI DSS 3–4 (2012), *available at* http://www.f5.com/pdf/white-papers/complying-pci-dss-wp.pdf.

[120] For example, according to a 2010 PCI DSS compliance study undertaken by Verizon, out of 200 organizations assessed, 49 percent were at least 90 percent PCI DSS compliant. *Verizon 2010 Payment Card Industry Compliance Report*, VERIZON 4, 7 (2010), *available at* http://www.verizonbusiness.com/resources/reports/rp_2010-payment-card-industry -compliance-report_en_xg.pdf.

[121] *See supra* Part II.B.

[122] *See supra* Part III.

[123] *See* Rustad & Koenig, *Extending*, *supra* note 4, at 239–40.

[124] *See Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*, PCI SEC. STANDARDS COUNCIL, *supra* note 36, at 5.

[125] For the problems with using HIPPA or the GLBA as the basis for a negligence per se cause of action, see Rustad & Koenig, *The Tort*, *supra* note 5, at 1594–97.

C. Causation

As with many negligence causes of action, the basic argument for causation in this context should be that, but for a company's failure to comply with the legislated standards and properly secure consumer data, the plaintiff's data would not have been exposed, thereby causing injury to the plaintiff.[126] The Restatement (Second) of Torts section 431 states that: "The actor's negligent conduct is a legal cause of harm to another if (a) his conduct is a substantial factor in bringing about the harm."[127] As Rustad and Koenig rightly point out, "[i]t may be difficult to determine whether a software bug, security hole, or a misconfiguration was a 'substantial factor' if the security breach was connected to multiple potential causes."[128] Ideally, this should be an issue for the finder of fact to resolve.[129] The plaintiff in this type of negligence per se data breach case should be able to begin by pointing to a part of the defendant company's (the company holding the consumer's data) security that failed to meet the legislative standards. The burden should then be on the defendant company to provide a reason as to why a third party in charge of that particular piece of software or security component is really the one responsible for the flaw.[130]

D. Harm and Damages

As a result of the ethereal nature of data breaches, consumers do not suffer the physical injuries that plague many unfortunate tort victims.[131]

---

[126] For this argument in the software context, see Rustad & Koenig, *The Tort*, *supra* note 5, at 1600–01 ("In a negligent enabling case, a plaintiff will need to demonstrate a causal connection (cause-in-fact) between software defects and consequential or direct damages suffered .... The 'but-for' test would determine 'whether the defendant's conduct was a cause in fact of the plaintiff's harm.'" (footnote omitted)).

[127] RESTATEMENT (SECOND) OF TORTS § 431 (1965); *see also* Rustad & Koenig, *The Tort*, *supra* note 5, at 1601 ("The Restatement (Second) of Torts adopted a 'substantial factor' test that only requires that the defendant materially contribute to a computer intrusion or internet security breach.").

[128] Rustad & Koenig, *The Tort*, *supra* note 5, at 1601.

[129] *See id.* at 1602 ("In a computer security case, the plaintiff must present facts and circumstances that will convince a jury that the cybercrime that caused the plaintiff's injury was facilitated by the data handler or software vendor.").

[130] For an example of this argument in the context of HIPPA, see *id.* at 1595 ("Health care providers punished for such unauthorized disclosures of individually identifiable health information should be able to seek indemnification against a software vendor whose products or services paved the way for the wrongful disclosure.").

[131] *See* Rustad & Koenig, *The Tort*, *supra* note 5, at 1603 ("The predominant injury in a cybertort case will be a financial loss, dignitary injury, or invasion of privacy rather than personal injury or death.").

The data breach victim suffers harm in the form of "increased risk of identity fraud, fear of identity fraud, and cost of efforts to reduce their risk of identity fraud," analogous to the toxic tort categories of "enhanced risk, fear of future harm, and medical monitoring."[132] Arguments on these theories of harm have failed to gain much traction in the courts.[133] Enhanced risk is hard for plaintiffs to prove as a matter of mathematical probability—the correlation between information obtained from data breach and actual instances of identity theft is surprisingly low, comprising only 1.5% to 4% of all identity theft reports.[134] Fear of future harm falls into the category of emotional harms courts have found "too speculative to confer standing."[135] Costs of efforts to reduce the risk of actual identity theft, generally in the form of credit monitoring services,[136] are seen as distinguishable from medical monitoring costs in toxic tort cases. Credit monitoring is seen as a preventive measure, to avoid future theft from intervening third-party use of the stolen data, whereas medical monitoring costs are seen as efforts at early diagnosis and treatment of a more likely medical harm.[137] All of these problems lead to conclusions like that of Judge Ripple in the Seventh Circuit

---

[132] James Graves, *"Medical" Monitoring for Non-Medical Harms: Evaluating the Reasonable Necessity of Measures to Avoid Identity Fraud After a Data Breach*, 16 RICH. J.L. & TECH. 2, 5–6 (2009).

[133] *See id.*; Rustad & Koenig, *Extending*, *supra* note 4, at 264 ("No plaintiff has been successful in receiving an award to compensate for lost data where identify theft has not yet occurred.").

[134] *See* Schneider, *supra* note 12, at 288 (citing Steve Lohr, *Surging Losses, but Few Victims in Data Breaches*, N.Y. TIMES, Sept. 27, 2006, http://www.nytimes.com/2006/09/27/technology/circuits/27lost.html).

[135] Graves, *supra* note 132, at 6 (citing Ponder v. Pfizer, Inc., 522 F. Supp. 2d 793, 796–98 (M.D. La. 2007) (dismissing plaintiff's claims, including fear and apprehension of fraud, on the grounds they did not constitute recoverable damages)); Randolph v. ING Life Ins. & Annuity Co., 486 F. Supp. 2d 1, 8–9 (D.D.C. 2007) (holding that plaintiffs' claim of substantial risk of harm of identity theft failed to amount to more than speculation); Forbes v. Wells Fargo Bank, N.A., 420 F. Supp. 2d 1018, 1020–21 (D. Minn. 2006) (granting defendant company's motion for summary judgment on plaintiff's failure to articulate present injury); Guin v. Brazos Higher Educ. Serv. Corp., Inc., No. CIV. 05-668 RHK/JSM, 2006 WL 288483, at *3–6 (D. Minn. Feb. 7, 2006) (holding plaintiff's claim deficient for failing to provide evidence that data was ever held or used with intent to commit unlawful activity).

[136] *See* Vincent R. Johnson, *Credit-Monitoring Damages in Cybersecurity Tort Litigation*, 19 GEO. MASON L. REV. 113, 113 (2011) ("In this type of arrangement, a business reviews information, generally on a daily basis, from one or more of the major credit-reporting agencies. When a change in the data subject's credit history occurs, such as the unauthorized opening of a new account in the victim's name, the service alerts the [victim].").

[137] *See* Graves, *supra* note 132, at 28.

case *Pisciotta v. Old National Bancorp*,[138] that "[w]ithout more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy."[139]

There is no simple solution to this "present injury"[140] barrier that data breach plaintiffs face in pursuing their claims. In some sense, courts need to come around to the idea that simply having your data in unauthorized hands, outside of your control, is an injury that occurs entirely separate from actual fraudulent transactions.[141] While the readily measurable costs of this injury may be small, in the form of credit monitoring costs (often provided by the breached company anyway, in an effort to build goodwill after a breach)[142] and costs to secure replacement financial and identification cards such as driver's licenses, there is also an emotional component not captured in these costs. Plaintiffs deserve the recognition of the fact that they now have to deal with the overhanging fear that they will transition from data breach victims to full-blown identity theft victims[143] and the fact that they were let down by a company they entrusted with their sensitive data as a present, immediate, and compensable injury.

Assuming the present injury barrier can be overcome, plaintiffs face another hurdle in the form of the Economic Loss Rule.[144] In short, the Economic Loss Rule operates to preclude recovery when the parties have a

---

[138] Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 640 (7th Cir. 2007).

[139] *Id.* at 639.

[140] *See* Rustad & Koenig, *Extending*, *supra* note 4, at 264–66 (discussing the present injury barrier as an obstacle plaintiffs face in pursuing their claims when data breach has resulted in a loss of their data yet no actual identity theft has occurred).

[141] *See* Johnson, *supra* note 136, at 141.

[142] *Id.* at 125–28 (citing numerous examples of breached companies providing anywhere from one to three years of free credit monitoring to affected consumers, including Sony in the PlayStation breach discussed in Part I.B). Indeed, as a result of increased incentive presented by the kind of suits proposed by this Note, virtually all companies may come to automatically provide credit monitoring costs. This should not preclude action however, because credit monitoring does nothing to ease consumer fear of actual identity theft that may not appear on credit reports, such as opening accounts or obtaining services that do not require a credit check. *See Defend: Recover from Identity Theft*, FED. TRADE COMM'N, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/defend.html (last visited Feb. 2, 2013).

[143] Indeed, this overhanging fear is precisely why commentators analogize data breach victims to medical monitoring cases. *See* Rustad & Koenig, *Extending*, *supra* note 4, at 264–65 ("The victims of a widespread data theft such as the TJX case could form a 'monitoring class' roughly paralleling consumers implanted with a defective medical device that has not yet injured them.").

[144] *Id.* at 268 & n.139 (pointing out that even if the present injury barrier can be overcome, "courts permit no recovery for purely economic losses" and that "plaintiffs have not been successful in side-stepping the ELR in negligent data handling cases").

direct contractual relationship and damages are consequential (lost profits), rather than direct (property damage or personal injury).[145] As Vincent Johnson persuasively argues, however:

> In large measure, the economic loss rule is intended to further the private ordering of business transactions. However, data-security statutes in many states hold that private agreements disclaiming legislatively imposed obligations related to computerized personal information are not enforceable and are void as against public policy. Consequently, the duties at issue in cybersecurity cases are, in large measure, not a proper subject for private ordering. For this reason ... the economic loss rule should not foreclose recovery of credit-monitoring damages.[146]

Unfortunately, as Johnson points out, not all courts have adopted this view in data breach cases.[147]

If, however, plaintiffs can successfully overcome both the present injury and economic loss rules, their damages should not be limited merely to recovery of credit monitoring costs[148] and similar compensatory items. Perhaps more importantly, punitive damages should also be available to data breach plaintiffs. Data breach represents the perfect scenario for one of the basic rationales behind punitive damages: incentivizing citizens to bring suit when compensatory harm is relatively low but we, as a society, still wish to punish the harmful activity.[149] Additionally, punitive damages would serve a function of tort law that is often left behind in modern jurisprudence: the public expression of outrage at the actions of the tortfeasor.[150]

---

[145] *Id.* at 267; *see also* Johnson, *supra* note 136, at 122.

[146] Johnson, *supra* note 136, at 122–23 (footnotes omitted); *see also* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1816 (2010) ("These financial injuries have much in common with economic harm long redressed under other branches of tort law.").

[147] Johnson, *supra* note 136, at 123 (citing Paul v. Providence Health System–Oregon, 240 P.3d 1110 (Or. Ct. App. 2010) (holding that data breach plaintiffs could not recover credit monitoring costs because they constituted purely economic damages)).

[148] *But see* Graves, *supra* note 132, at 50–58 (arguing that an economic analysis assuming even the most expensive costs of actual identity theft and the highest probability of actual identity theft occurring suggests that it is not economically rational to purchase credit monitoring in the case of data breach).

[149] *See, e.g.*, Catherine M. Sharkey, *Punitive Damages as Societal Damages*, 113 YALE L.J. 347, 366–67 (2003).

[150] *See* Atl. Sounding Co. v. Townsend, 557 U.S. 404, 409 (2009) ("Damages are designed not only as a satisfaction to the injured person, but likewise as a punishment to the guilty, to deter from any such proceeding for the future, and as a proof of the detestation of the jury to the action itself" (quoting Wilkes v. Wood, 98 Eng. Rep. 489, 498–99 (C.P. 1763))).

CONCLUSION

As it stands today, consumer protection and relief after the fact from data breach is woefully inadequate. Companies are left to their own devices when it comes to securing sensitive consumer information, and as a result they often create systems that practically beg to be exploited by savvy hackers. The time is ripe for the federal government to step in and level the playing field by carefully constructing standards that allow consumers to have confidence that the companies with which they choose to do business are using reasonable and effective methods to secure their data.[151] Should that confidence prove misplaced, however, and should companies slip under the enforcement radar, consumers should not be left to bear the cost. By allowing consumers to hold companies like Sony and TJX accountable for negligent data security practices, we add another layer of incentive for companies to meet their duty of care. Consumers should not be denied access to courts merely because some unknown third party has not used their data in a detrimental way. The fact is that when consumer data is stolen, it is stolen from consumers, not the companies holding the data. It is at that point that consumers have suffered an injury, and it is at that point they should be allowed to hold responsible the company that made that injury possible.

John A. Fisher[*]

[151] Indeed, the government itself may also have national security incentives to step into this arena. *See* Elisabeth Bumiller & Thom Shanker, *Panetta Warns of Dire Threat of Cyberattack on U.S.*, N.Y. TIMES, Oct. 11, 2012, https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all.

[*] J.D. Candidate, 2013, William & Mary Law School; B.A., 2010, Ithaca College. The author thanks Professor Jason M. Solomon for inspiring this Note by introducing him to civil recourse tort theory and instilling in him a focus on the individual's place in the law. The author would also like to thank Nicole Hartz for her constant encouragement and incredible culinary support. Finally, the author would like to thank the members of the 2012–2013 *William & Mary Business Law Review* for their hard work and immensely helpful suggestions throughout the Note writing process.